Introduction to Vendor Management

Catherine Tibaaga

Agenda

- Purpose and Definition of **Vendor Management**
- Why is **Vendor Management** Important?
- What is the **Vendor Management Life Cycle**?
- What is the **Planning Phase** of the Vendor Management Life Cycle?
- What is the **Due Diligence Phase** of the Vendor Management Life Cycle?
- What is the **Vendor Risk Assessment Process** in the **Due Diligence Phase**?
- What is the **Implementation and Onboarding Phase** of the Vendor Management Life Cycle?
- What is the **Performance Management and Monitoring Phase** of the Vendor Management Life Cycle?
- What is the **Termination Phase** of the Vendor Management Life Cycle?
- Conclusion
- Summary
- Thank You

Purpose and Definition of Vendor Management

- Objective:
  - Understand the principles that govern a Vendor Management program within an organization.

- What is Vendor Management?
  - Vendor Management is the practice of managing activities associated with outsourcing functions and processes to outside entities.

Why is Vendor Management Important?

- Many organization choose to outsource to outside entities such as vendors and suppliers for the following reasons:
  - To improve efficiency in processes and functions
  - To enable cost savings
  - To comply with regulations by utilizing vendors that provide specialized services

- Despite the benefits of outsourcing to vendors, there exist risks that could undermine the strategic objectives of the organization.

- To properly manage and control the risks associated with outsourcing, organizations should implement and maintain a vendor management program.

What is the Vendor Management Life Cycle?

- *Vendor Management is the practice of controlling activities associated with outsourcing functions and processes to outside entities.*

- A Vendor Management program should include a **Vendor Management Life Cycle** in order to manage activities associated with outsourcing**.**

- The **Vendor Management Life Cycle** consists of the following phases listed below:
  - **Planning**
  - **Due Diligence**
  - **Implementation and Onboarding**
  - **Performance Management and Monitoring**
  - **Termination**

What is the Planning Phase of the Vendor Management Life Cycle?

- The Planning Phase of the Vendor Management Life Cycle allows the business to determine the benefits and drawbacks of outsourcing a function or process to a vendor.

- As part of the Planning Phase, the business should conduct a *Cost-Benefit Analysis* to determine whether it is more cost effective for the business to outsource to a vendor or to perform the services in-house.
  - A *Cost-Benefit Analysis* is a process where the business evaluates the potential rewards and potential costs and losses associated with a business activity such as outsourcing to a vendor.
  - The *Cost-Benefit Analysis* should include a budget for outsourcing versus a budget for performing the services in-house.
  - The *Cost-Benefit Analysis* should also describe whether in-sourcing or outsourcing leads to greater accuracy and efficiency in business functions and processes.
  - If the *Cost-Benefit Analysis* proves that it is beneficial for to the business to outsource a specific function or process to a vendor, then the business has a business case for outsourcing.

What is the Planning Phase of the Vendor Management Life Cycle?

- In addition to performing a *Cost-Benefit Analysis*, the business should develop a *Scope of Work (SOW)* which includes the business activities that the vendor is to complete.
  - The business should leverage the *Standards of Operating procedures (SOPs)* for the function or process that they wish to outsource in order to draft the *SOW*.
  - *A SOW is a document that explains the tasks that the vendor is to complete for the business*.
  - *A SOP* is a *set of written instructions that describes the step-by-step process that must be taken to properly perform a routine activity.*
- Once the *Cost-Benefit Analysis* is completed, the business should identify a list of vendors that provide the products/services that the business wishes to obtain.
  - To identify the list of vendors that provide the products/services the business wishes to procure, the business can conduct a search on the various vendors that provide the products/services.

What is the Planning Phase of the Vendor Management Life Cycle?

- Once the business has identified a list of vendors that provide the products/services they wish to obtain, the business should research the vendors in order to find any news events associated with the vendors.
  - A *news events search* should answer the following questions below for each vendor identified:
    - *Has the vendor experienced any information security breaches within the last ten years?*
    - *Has the vendor filed for bankruptcy within the past 10 years?*
    - *Has the vendor been involved in any lawsuits or legal disputes within the last ten years?*
      - *Has the vendor paid restitution as a result of the lawsuits and legal disputes?*
    - *Has the vendor been subjugated to regulatory penalties due to not following regulatory requirements?*
  - To perform the *news event search*, the business can utilize a search engine (i.e. Google) or they can utilize a technological solution (i.e. Dun and Bradstreet, LexisNexis).
- Once the *Cost-Benefit Analysis, the SOW* and the *news event search* are completed, the business should prepare a *Request-For-Proposal (RFP)* that they will submit to the vendors.
  - A *RFP* is a document that the business will submit to the vendors requesting that the vendors submit specific information in order for the business to determine which vendor fits the criteria necessary to provide products/services to the business.

What is the Planning Phase of the Vendor Management Life Cycle?

When sending a *RFP* to various vendors, the *RFP* should ask that the vendors provide the following information:

- *Quotes:* The vendors should provide pricing based on the *SOW* provided by the business in the *RFP*.
- *Vendor Financial Statements:* The vendors should submit their financial statements in order for the business to evaluate their financial health and profitability.
  - Financial statements include the *Income Statement*, the *Statement of Capital*, and the *Balance Sheet*.
- *Certificates of Insurance (COI):* The vendors should provide copies of their COIs to show that they have business insurance.
- *Information regarding the vendors' internal controls in the following risk areas: Information Security, Privacy, Business Continuity, Disaster Recovery, Compliance with Industry Standards and Regulation.*
  - In order to obtain information from the vendors regarding their internal controls, the business should include in the *RFP* a *Preliminary Due Diligence Questionnaire (DDQ)* for the vendors to complete.
  - The *Preliminary DDQ* should be drafted and approved by the various risk subject-matter experts (SMEs) from the following risk areas: Information Security, Privacy, Business Continuity, Disaster Recovery, and Compliance.

What is the Planning Phase of the Vendor Management Life Cycle?

- For a sample *Preliminary DDQ*, refer to the **Sample Preliminary Due Diligence Questionnaire (DDQ)** at **www.catherinetibaaga.com/resources**.

- Once the vendors provide the requested documents to the business, the business should evaluate all the information provided by the vendors to determine which vendor to select for the **Due Diligence Phase** of the Vendor Management Life Cycle.
  - When evaluating the vendors, the business should review and analyze the following information below:
    - **Pricing:** Which vendor offers the best pricing that fits within the company budget for outsourcing?
    - **Financial:** Which vendor is the most financially healthy and profitable after analyzing their financial statements?
    - **Risk Management:** Which vendor has the most effective basic internal controls to manage and control risks?
      - The business should work with the risk subject-matter experts to evaluate the Preliminary DDQs for each vendor and determine which vendor has sufficient internal controls to manage and control risks.
    - **COIs:** Which vendor has sufficient insurance coverage?
      - To determine what constitutes sufficient coverage, the business should establish what is the minimum insurance coverage that a vendor must have in order to engage with the business.
    - **News Events:** Which vendor has the least negative news events?

What is the Planning Phase of the Vendor Management Life Cycle?

- Prior to sending a *RFP* to vendors, The business should send the vendors a *Non-Disclosure Agreement (NDA)* in order to protect the confidentiality of information exchanged between the vendors and the business.

- If the business chooses to not conduct a *RFP*, the business can also consider only one vendor. The purpose of conducting an *RFP* is to ensure that the business selects the best vendor that is offering the most competitive price.
  - If the business decides to only consider one vendor, then the business should create a written justification for why the business chose to only consider one vendor versus submitting a *RFP* to various vendors.

  - When considering only one vendor, the business should request the same information below from the vendor in order to determine if they qualify to provide products/services to the business.
    - **Pricing:** The vendor should provide pricing based on the *SOW* provided by the business.

    - **Financial Statements:** The vendor should provide their financial statements in order for the business to determine if they are financially healthy and profitable.
      - Financial statements include the *Income Statement*, the *Statement of Capital*, and the *Balance Sheet*.

What is the Planning Phase of the Vendor Management Life Cycle?

- **Preliminary DDQ:** The vendor should complete a Preliminary DDQ provided by the business. The Preliminary DDQ includes basic questions related to risk management in the following areas: *Information Security, Privacy, Business Continuity, Disaster Recovery and Compliance.*

- **COIs:** The vendor should provide a COI as proof that they have adequate business insurance.
  - To determine what constitutes sufficient coverage, the business should establish what is the minimum insurance coverage that a vendor must have in order to engage with the business.

- Similar to conducting a *RFP*, the business should conduct a *news event search* on the vendor to determine if the vendor has experienced any negative events that have impacted their business.
  - A *news events search* should answer the following questions below:
    - *Has the vendor experienced any information security breaches within the last ten years?*
    - *Has the vendor filed for bankruptcy within the past 10 years?*
    - *Has the vendor been involved in any lawsuits or legal disputes within the last ten years?*
      - *Was the vendor expected to pay restitution as a result of the lawsuits and legal disputes?*
    - *Has the vendor been subjugated to regulatory penalties due to not following regulatory requirements?*

What is the Planning Phase of the Vendor Management Life Cycle?

- Prior to requesting information from one vendor, the business should send a *NDA* to the vendor to protect the confidentiality of information exchanged between the business and vendor.

- Once the business completes the evaluation process, the business should select a vendor if the vendor was part of a *RFP*.

- Once a vendor is selected, the business can move forward to the **Due Diligence Phase of the Vendor Management Life Cycle**.

What is the Due Diligence Phase of the Vendor Management Life Cycle?

- The Due Diligence Phase of the Vendor Management Life Cycle requires that the business undergo a vendor risk assessment. The purpose of the vendor risk assessment is to determine if the selected vendor has sufficient internal controls to protect the business from the following types of risks listed below:
  - Financial Risk
  - Reputational Risk
  - Information Security Risk
  - Privacy Risk
  - Compliance Risk
  - Business Continuity Risk
  - Disaster Recovery Risk

What is the Vendor Risk Assessment Process in the Due Diligence Phase?

- The vendor risk assessment process requires that the business complete the following steps below:
  - Identify *inherent risks* associated with outsourcing the function or process.
    - *Inherent risks* represent the probability or likelihood of material and monetary losses without taking into consideration compensating controls in place to protect the organization.
    - To identify *inherent risks*, the business should utilize an *inherent risk questionnaire* that produces an inherent risk score.
      - For a **Sample Inherent Risk Questionnaire**, refer to the sample at **www.catherinetibaaga.com/resources**.
    - The inherent risk score represents the level of criticality associated with the outsourced function or process.

What is the Vendor Risk Assessment Process in the Due Diligence?

- Once an inherent risk score is produced, the business should determine the type of risk assessments to send to the vendor based on the inherent risk score. The risk assessments should include the following below:
  - **Financial Risk Assessment:** Determines if a vendor possesses the ability to earn adequate income, pay its debts and reward shareholders. To complete a financial risk assessment, the business can analyze the financial statements of the vendor.
    - The business can leverage the results of the financial statement analysis conducted during the *Planning Phase of the Vendor Management Life Cycle* to complete the financial risk assessment.
    - Financial statements include the *Income Statement*, the *Statement of Capital* and the *Balance Sheet*.
  - **Reputational Risk Assessment:** Determines if a vendor has been subject to negative publicity or public perception. To conduct a reputational risk assessment, the business can conduct an internet search or utilize technological solutions such as Dun and Bradstreet or LexisNexis.
    - The vendor can utilize the results of the news event search conducted during the *Planning Phase of the Vendor Management Life Cycle.*

What is the Vendor Risk Assessment Process in the Due Diligence?

- Determine the type of risk assessments to send to the vendor based on the inherent risk score. The risk assessments should include the following below:
  - **Information Security Risk Assessment:** Determines if a vendor possesses adequate internal controls to prevent the unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of information.
  - **Privacy Risk Assessment:** Determines if a vendor possesses adequate internal controls to prevent the unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of consumer personal data such *Personal Identifiable Information (PII)* and/or *Personal Health Information (PHI).*
    - *PII* applies to institutions that are subject to Privacy Laws such as the Glamm-Bleach Bliley Act (GLBA) and/ or General Data Protection Regulation (GDPR).
    - *PHI* applies to institutions that are subject to Privacy Laws such as Health Insurance Portability and Accountability Act of 1996 (HIPAA).

What is the Vendor Risk Assessment Process in the Due Diligence Phase?

- Determine the type of risk assessments to send to the vendor based on the inherent risk score. The risk assessments should include the following below:
  - **Compliance Risk Assessment:** Determines if the vendor adheres to applicable industry regulations, laws or industry standards.
  - **Business Continuity Risk Assessment:** Determines if the vendor possesses adequate controls to provide services or products to the organization and meet their contractual Service Level Agreements (SLAs) in the event of a business disruption.
  - **Disaster Recovery Risk Assessment:** Determines if the vendor possesses adequate controls to ensure that vital technological systems, infrastructure and information is recoverable due to a natural or man-made disaster.

What is the Vendor Risk Assessment Process in the Due Diligence Phase?

- Once the vendor completes the vendor risk assessments, they should provide their responses with supporting documentation back to the business to review.

- The business should analyze and evaluate the vendor risk assessments along with the supporting documentation to determine the *residual risks* associated with the vendor.
  - *Residual risk* represents the probability or likelihood of material and monetary losses taking into consideration compensating controls in place to protect the organization.

- The business should provide the results of the vendor risk assessment to the vendor in the form of a *Risk Mitigation Action Plan (R-MAP)*.

- The *R-MAP* should contain all of the information security, business continuity, disaster recovery, financial, compliance and reputational risks identified during the vendor risk assessment.

- The vendor should work with the business to mitigate all risks identified in the *R-MAP*.

What is the Vendor Risk Assessment Process in the Due Diligence and Selection Phase?

- Once the risks are mitigated, the business can move forward to the **Implementation and Onboarding Phase of the Vendor Management Life Cycle.**

- All risks identified during the vendor risk assessment process should be monitored and reported to Enterprise Risk Management and/or Operational Risk Management as required by the **Three Lines of Defense Model.**

- Please refer to **The Importance of Third-Party Risk Assessments for Financial Institutions** at **www.catherinetibaaga.com/resources** for more information about vendor risk assessments**.**

What is the Implementation and Onboarding Phase of the Vendor Management Life Cycle?

- The Implementation and Onboarding Phase of the Vendor Management Life Cycle requires that the business execute the contract with the selected vendor in order for the business to utilize them.

- As a best practice, the business should ensure that all risks identified during the vendor risk assessment are properly mitigated by the vendor prior to executing a contract with the vendor.
  - If the business needs to execute the contract prior to the vendor mitigating all risks identified during the vendor risk assessment process, the business should add proper language to the contract (i.e. right-to-audit and remediate) to ensure that the vendor mitigates all risks identified within a specific time frame.

- The business should ensure that the contract includes contractual language that addresses vendor risks (i.e. *information security, business continuity, disaster recovery, compliance with applicable industry standards and regulations).*
  - If the vendor will receive PII and/or PHI, the contract should also include contractual language that ensures that the vendor adheres to privacy laws (i.e. GLBA, HIPAA, GDPR).

What is the Implementation and Onboarding Phase of the Vendor Management Life Cycle?

- When drafting the contract, the business should ensure that the contract includes the appropriate *Service Level Agreements (SLAs)* and performance requirements.
  - *SLAs are the expectations set by the business on the type and quality of service that the vendor is to provide to the business.*
  - *SLAs* should include performance metrics that enable the business to measure vendor performance.
  - In the event that the vendor cannot meet the performance expectations, the contract should state the penalties for poor performance.
- The business should also ensure that the contract includes standard contractual language that addresses the following terms and conditions:
    - **Indemnification**: Specifies the extent to which the organization will be held liable for claims when the vendor fails to perform.
    - **Right-to-Audit and Remediate**: Ensures that the business can audit and monitor the performance of the vendor. The vendor should remediate all findings as a result of an audit within a specific time frame. For example, vendor risk assessments serve as an example of an audit where the vendor is obligated to remediate all risk finding identified during the audit.

What is the Implementation and Onboarding Phase of the Vendor Management Life Cycle?

- The business should also ensure that the contract includes standard contractual language that addresses the following terms and conditions:
  - **Limits of Liability:** Limits the level of exposure the business will face in the event of a claim or lawsuit filed against the business. In the event it is enforced, the clause will essentially limit how much the vendor is required to pay in damages should they be held responsible for failing to perform according to the contract.
  - **Insurance:** Specifies how much insurance the vendor should carry in order to protect the business. The vendor should provide a Certificate of Insurance (COI) to the business as proof of insurance.
  - **Dispute Resolution:** Specifies the arbitration and remediation process in order to resolve issues between the vendor and the business.
  - **Default and Termination:** Specifies what constitutes a failure of the vendor to meet contractual obligations and the conditions for ending the contract.

What is the Implementation and Onboarding Phase of the Vendor Management Life Cycle?

- The business should also ensure that the contract includes standard contractual language that addresses the following terms and conditions:
    - **Subcontracting:** Dictates whether the vendor can outsource the activities that it performs for the business to an outside entity. If the contract allows subcontracting, the contract should dictate how the vendor is supposed to manage the fourth-party/subcontractor and how they plan to communicate with the business whether the fourth-party performs adequately.
        - If a subcontractor is allowed, the business should ensure that the vendor has an adequate vendor management program that enables them to successfully monitor the performance of the fourth-party/subcontractor.
    - Any other terms and conditions that the vendor needs to follow.
- Once the contract is executed with the vendor, the business should also create an *exit strategy* and *contingency plan.*
    - An *exit strategy* is plan that outlines all the activities that the business and vendor must complete to successfully transition the services to another vendor or terminate the business relationship with the current vendor.
    - The business should work with information security, business continuity and disaster recovery to draft the exit plan.

What is the Implementation and Onboarding Phase of the Vendor Management Life Cycle?

- The business should collaborate with the business units and other stakeholders (i.e. information security) to ensure that the *exit strategy* describes how the vendor should return or destroy data that they received from the business.

- In addition to an exit strategy, the business should also work with the business units and other stakeholders (i.e. *information, security*, business continuity and disaster recovery) to create a *contingency plan* in the event that the vendor fails to meet its Service Level Agreements (SLAs).
  - A *contingency plan* is a document that outlines how the business should respond in the event of a business disruption that prevents the vendor from meeting its SLAs and contractual obligations.

What is the Performance Management and Monitoring Phase of the Vendor Management Life Cycle?

- Once the contract is executed, the business can start to utilize the vendor.

- As part of the vendor management life cycle, the business should monitor and manage vendor performance to ensure that the vendor meets their contractual obligations to the business.

- To monitor vendor performance, the business should conduct performance meetings on a periodic basis with the vendor to ensure that the vendor meets their Service Level Agreements (SLAs).
    - The frequency of the performance meetings depends on the inherent risk score assigned to the vendor. For example, the business should conduct performance meetings with critical vendors on a monthly basis.

    - For non-critical vendors, the business should conduct performance meetings either on a quarterly, semi-annual or annual basis.

What is the Performance Management and Monitoring Phase of the Vendor Management Life Cycle?

- In addition to conducting performance meetings, the business should complete *Key Performance Indicators (KPIs)* on a consistent basis to monitor vendor performance.
  - The purpose of conducting KPIs is to capture whether the vendor met their contractual obligations and SLAs.
  - *A KPI is a tool that measures and evaluates the success of specific objectives and activities*.
  - Completing KPIs is a risk mitigation activity that enables the business to determine if the vendor can adequately perform the services as dictated by the contract.
- In the event the business identifies performance issues when completing the KPIs, the business should receive an *Issue Mitigation Plan* from the vendor on how they plan to solve the issues identified and prevent further performance issues.
  - Performance issues with vendors that are not mitigated expose the vendor and ultimately the business to operational and contract risk that could lead to financial and reputational losses for the business and the vendor.
  - The business should also work with Operational Risk Management or Enterprise Risk Management to report any issues that classify as information security, business continuity, disaster recovery, financial, reputational and compliance issues.

What is the Termination Phase of the Vendor Management Life Cycle?

- If the business decides to no longer utilize the vendor, the business should leverage the *Exit Strategy* to offboard the vendor.
  - The *exit strategy* should include the vendor offboarding checklist that ensures that the business and the vendor complete specific activities in order to successfully terminate or transition the vendor relationship.
  - The business should also refer to the termination clause in the contract to properly terminate the contract with the vendor.
  - The business should work with information security and privacy to ensure that the vendor properly destroys or returns all data that was provided to them.
    - If the vendor plans on destroying the data, they should provide a *certificate of destruction* to the business once the data is destroyed.
    - If the vendor cannot destroy the data, the business should enforce the contractual language regarding *records retention*.

Conclusion

Summary

- When choosing to outsource functions or processes to vendors, the business should ensure that they create, implement and maintain an effective vendor management life cycle.

- Creating, implementing and maintaining an effective vendor management life cycle ensures that the business can properly maximize the benefits of outsourcing while minimizing the risks.

Thank You

Catherine Tibaaga

www.catherinetibaaga.com