Third-Party Risk Management Program

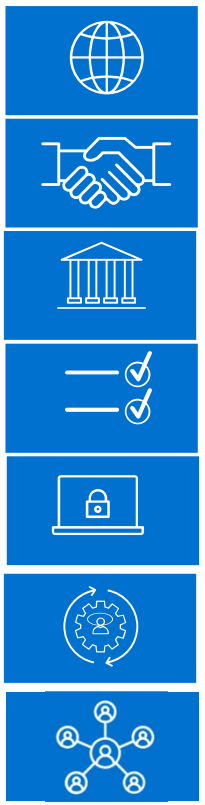
May 2021

AGENDA

- TPRM Overview
  - Risk Management Lifecycle
  - Assessing Risk
  - Planning
  - Due Diligence/Selection
  - Contract Negotiation
  - Termination
- Onboarding a Vendor
- Ongoing Due Diligence
- Vendor Payments from Trust Accounts
- Signs of Ineffective Program

Third-Party Risk Management (TPRM)

There is not a one size fits all approach to TPRM but regardless of the structure, there should be key elements that are incorporated into the process.



- Strategic risk
- Reputational risk
- Credit risk
- Regulatory and compliance risk
- Information Security risk
- Operational risk
- Fourth Party Risk

Third-Party Risk Management (TPRM)

Risk Management Life Cycle

All organizations should implement risk management processes that are commensurate with the level of risk and complexity of its third-party relationships and the organization's organizational structures. Therefore, more comprehensive and rigorous oversight and management of third-party relationships are required which involve critical activities—significant functions (e.g., payments, clearing, settlements, custody) or significant shared services (e.g., information technology), or other activities that

- Could cause an organization to face significant risk if the third party fails to meet expectations.
- Could have significant customer impacts.
- Require significant investment in resources to implement the third-party relationship and manage the risk.
- Could have a major impact on operations if the organization has to find an alternate third party or if the outsourced activity has to be brought in-house.

Source: OCC

Third-Party Risk Management (TPRM)

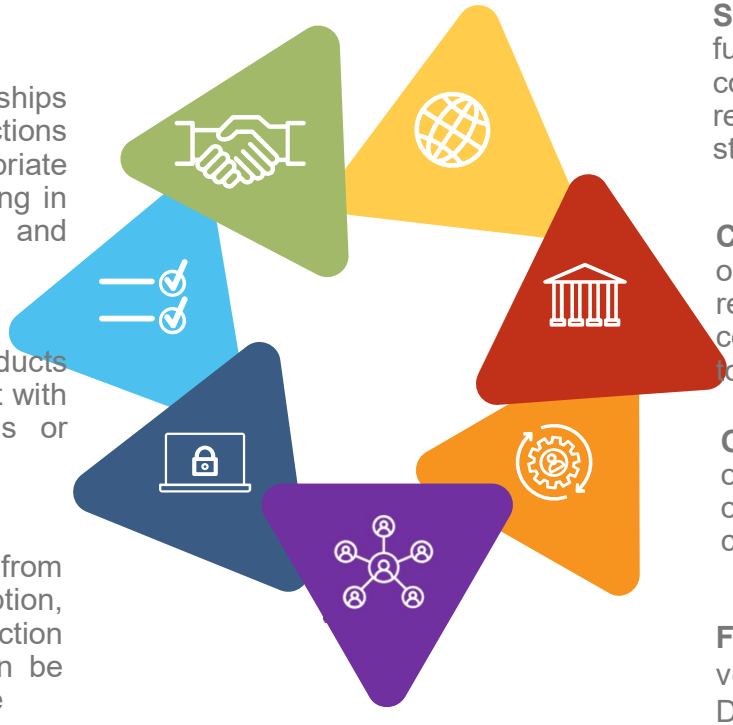
Assessment of Risk Posed by 3rd Party

In general, there are numerous risks that may arise from the use of third parties. Some of the risks are associated with the underlying activity itself, similar to the risks faced if the organization conducted the activity. Other potential risks arise from or are heightened by the involvement of a a third party. Failure to manage these risks can expose organizations to regulatory action, financial loss, litigation and damage, and may even impair the organization's ability to establish new or service existing customer relationships.

Reputational Risk: Third party relationships may result in dissatisfied customers, interactions not consistent with branch policies, inappropriate recommendations, security breaches resulting in the disclosure of customer information and violations of law and regulation.

Compliance Risk: Risk exists when the products or activities of a third party are not consistent with governing laws, rules, regulations, policies or ethical standards.

Information Security Risk: Risk arising from unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of information. It is a general term that can be used regardless of the form the data may take



Strategic Risk: The use of a third party to perform functions that do not help the organization achieve corporate strategic goals and provide an adequate return on investment exposes the organization to strategic risk.

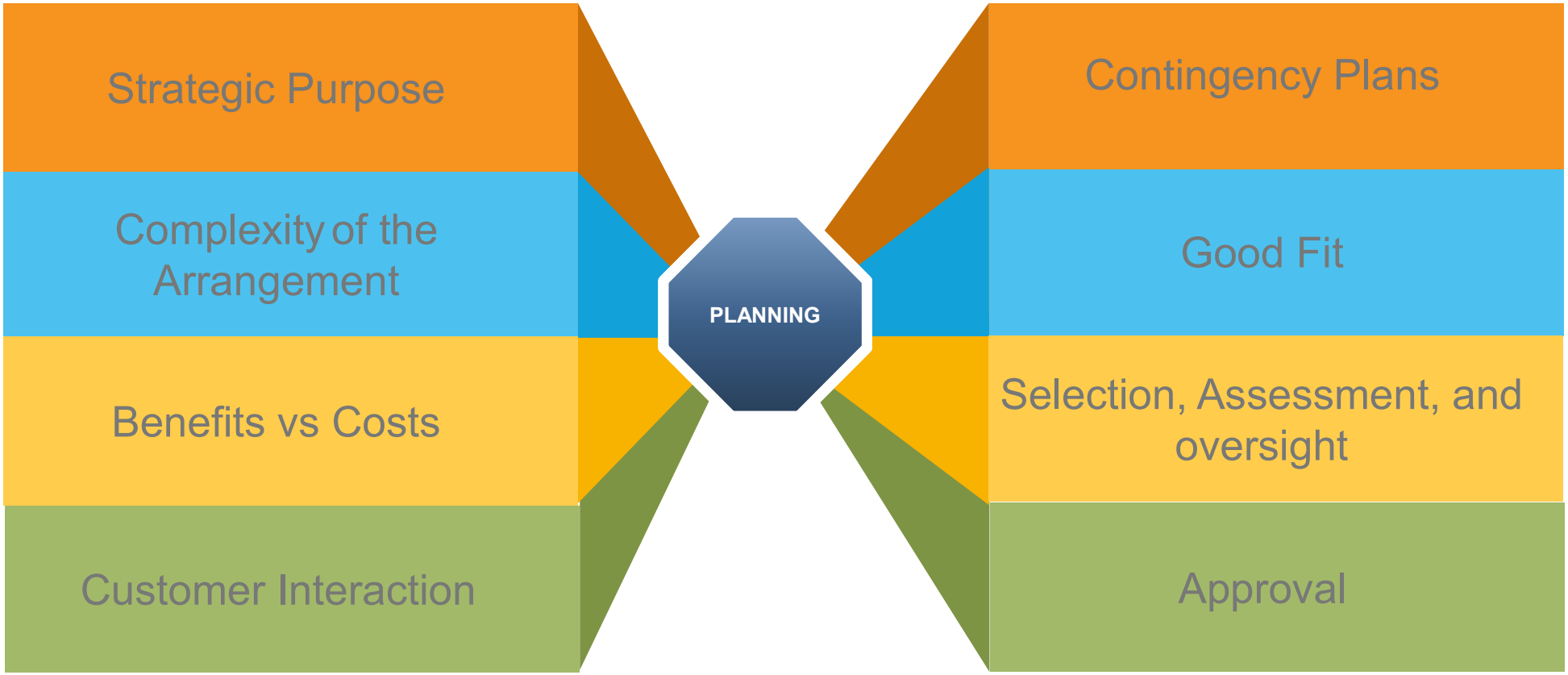
Credit Risk: Risk that a third party, or any other creditor necessary to the third-party relationship, is unable to meet the terms of the contractual arrangements with the organization or to otherwise financially perform as agreed.

Operational Risk: Third party relationships often integrate the internal processes of other parties with organization's processes and can increase the overall operational complexity.

Forth Party Risk: The risk that a third party vendor of your third party fails to perform. Does not make your company less responsible.

Planning

Before entering into a third-party relationship, senior management should develop a plan to manage the relationship. The management plan should be commensurate with the level of risk and complexity of the third-party relationship and should:



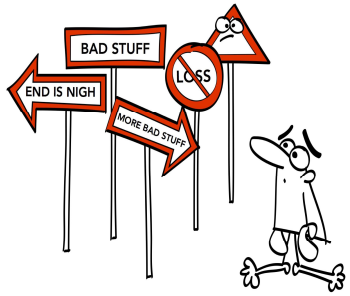
Due Diligence and Third-Party Selection

Regulatory Compliance

Financial Condition

Fee Structure

Risk Management



Information Security

Resilience

Insurance Coverage

Conflict of Interest

Contract Negotiation

Nature and Scope of Arrangement

A third-party contract should specifically identify the frequency, content, and format of the service, product, or function provided.

Performance Measures

Specify performance measures that define the expectations and responsibilities for both parties.

Frequency of Reporting

Provide and retain timely, accurate, and comprehensive information such as records and reports that allow management to monitor performance service levels, and risks..

The Right to Audit

Right to audit, monitor performance, and require remediation when issues are identified.

Responsibility for Compliance

Ensure the contract addresses compliance with specific laws, regulations, guidance, and self-regulatory standards applicable to the activities involved.

Cost and Compensation

Fully describe compensation, fees, and calculations for base services, as well as any fees based on volume of activity and for special requests.

Confidentiality and Integrity

Prohibit the third party and its subcontractors from using or disclosing the organization's information, except as necessary to provide the contracted activities or comply with legal requirements

Indemnification

Consider including indemnification clauses that specify the extent to which the organization will be held liable for claims that cite failure of the third party to perform..

Onboarding a New Vendor – Pre-Assessment

I. Factors to Consider
   A. Purpose of the Vendor's Service to the Institution
   B. Depth and Breadth of Service/Access to NPI
   C. Financial Health, Reputation and Applicable Insurance of the Vendor
   D. Reliance by the Vendor on 4th Parties
   E. Continuity of Service
   F. Available SOC Reports
II. Business Analysis
III. Contract Provisions/Legal Review
   A. Termination Provisions
   B. SLAs

Onboarding a New Vendor – Pre-Assessment

IV. Risk Assessment – how the institution could be impacted if the third party fails.
   A. Risks to be Evaluated
   B. Risk Exposure Assignment
   C. Mitigating Controls
   D. Final Assessment

V. Assignment of a Criticality Rating

VI. Implementation

VII. Post Implementation Review

Third-Party Risk Management (TPRM)

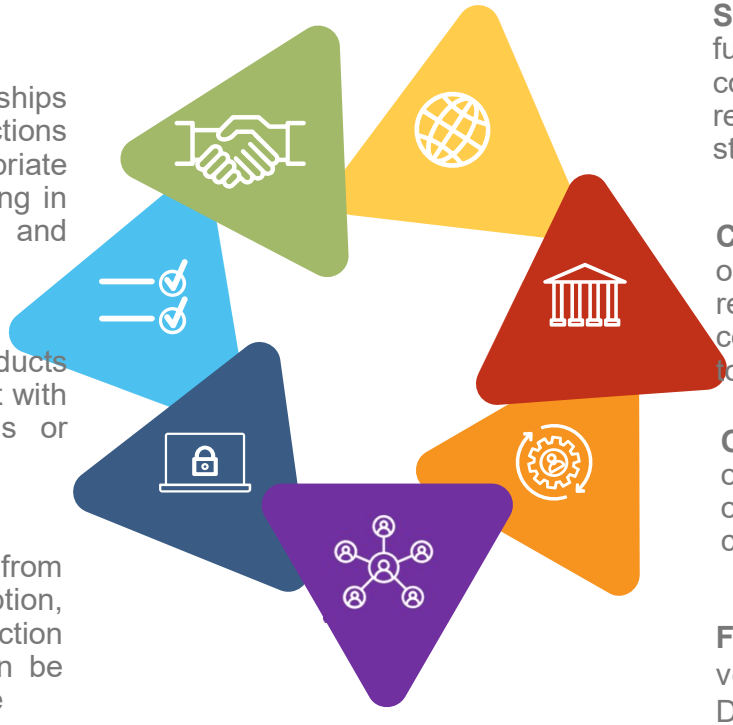
Assessment of Risk Posed by 3rd Party

In general, there are numerous risks that may arise from the use of third parties. Some of the risks are associated with the underlying activity itself, similar to the risks faced if the organization conducted the activity. Other potential risks arise from or are heightened by the involvement of a a third party. Failure to manage these risks can expose organizations to regulatory action, financial loss, litigation and damage, and may even impair the organization's ability to establish new or service existing customer relationships.

Reputational Risk: Third party relationships may result in dissatisfied customers, interactions not consistent with branch policies, inappropriate recommendations, security breaches resulting in the disclosure of customer information and violations of law and regulation.

Compliance Risk: Risk exists when the products or activities of a third party are not consistent with governing laws, rules, regulations, policies or ethical standards.

Information Security Risk: Risk arising from unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of information. It is a general term that can be used regardless of the form the data may take



Strategic Risk: The use of a third party to perform functions that do not help the organization achieve corporate strategic goals and provide an adequate return on investment exposes the organization to strategic risk.

Credit Risk: Risk that a third party, or any other creditor necessary to the third-party relationship, is unable to meet the terms of the contractual arrangements with the organization or to otherwise financially perform as agreed.

Operational Risk: Third party relationships often integrate the internal processes of other parties with organization's processes and can increase the overall operational complexity.

Forth Party Risk: The risk that a third party vendor of your third party fails to perform. Does not make your company less responsible.

Termination

A bank may terminate third-party relationships for various reasons, including:

- expiration or satisfaction of the contract.
- desire to seek an alternate third party.
- desire to bring the activity in-house or discontinue the activity.
- breach of contract.

Termination plan should cover the following:

Capabilities, resources, and the time frame

- Risks associated with data retention and destruction, information system connections and access control
- Handling of joint intellectual property developed during the course of the arrangement.
- Reputation risks to the bank if the termination happens as a result of the third party's inability to meet expectations.
- The extent and flexibility of termination rights may vary with the type of activity.

Ongoing Due Diligence for Existing Vendors

I. Frequency
II. Depth of Review
III. Considerations for Updated Documentations/Reviews
    A. Financial Review
    B. SLA Monitoring
    C. Insurance Requirements
    D. Prior Period Issues/Resolution of those issues
    E. Marketplace Information
    F. SOC Reports
    G. Contract Compliance

Matrix for Ongoing Due Diligence

I. Factors for Consideration
   A. Vendor Criticality Rating
   B. Vendor Risk Assessment Rating
   C. Levels of Due Diligence
II. Example:

	Risk Assessment - High	Risk Assessment - Low
Criticality – Critical	Annual Level 1 Due Diligence	Annual Level 1 Due Diligence
Criticality – High	Annual Level 2 Due Diligence; Level 1 Due Diligence every 2 Years	Annual Level 2 Due Diligence; Level 1 Due Diligence every 3 Years

Practical Application – Ongoing Due Diligence

I. Are all applicable documents (contract, NDA, etc.) up to date?
II. Evidence of continued policy enforcement/control framework (Current SOC-1 review)?
III. Analysis of Complementary User Controls within the Vendor SOC-1 to your organization's control framework?
IV. Any reported issues on the vendor within the media or public regulatory filings?
V. Are all parties operating in agreement with the contract/service level terms?
VI. Has anything changed with the vendor's access to NPI? Or direct contact with clients?

Practical Application – Ongoing Due Diligence

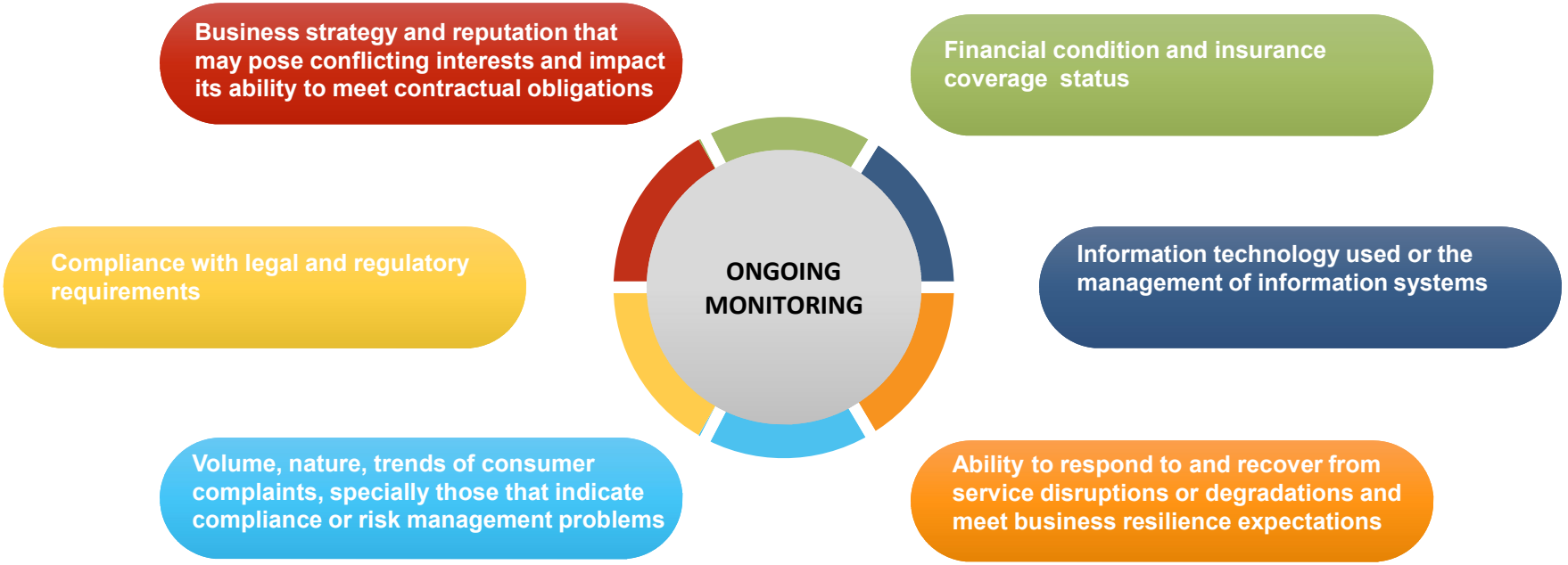
VII. Is there evidence of a recent Certificate of Insurance, if applicable?

VIII. If the financials are available, has a review been performed?

Ongoing Monitoring

Ongoing monitoring for the duration of the third-party relationship is an essential component of an organization's risk management process. More comprehensive monitoring is necessary when the third-party relationship involves critical activities. Senior management should periodically assess existing third-party relationships to determine whether the nature of the activity performed now constitutes a critical activity.

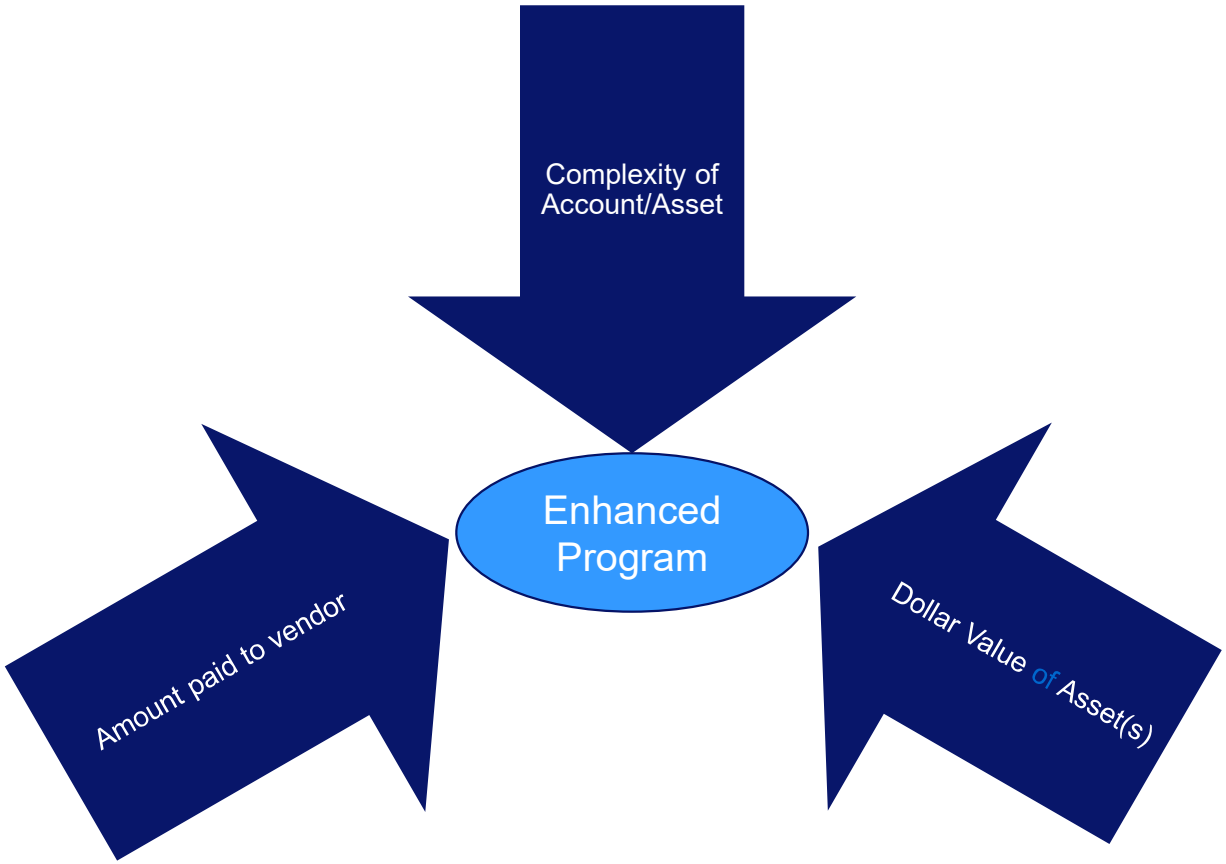
Because both the level and types of risks may change over the lifetime of third-party relationships, a bank should ensure that its ongoing monitoring adapts accordingly. This monitoring may result in changes to the frequency and types of required reports from the third party, including service-level agreement performance reports, audit reports, and control testing results. In addition to ongoing review of third-party reports, some key areas of consideration for ongoing monitoring may include assessing changes to the third party's:



Do you need a separate third-party risk management program?

DEPENDS

Vendor Payment from Trust Accounts



What should the program look like?

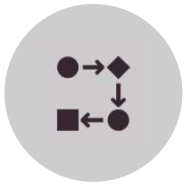
- Planning
- Risk Rating Methodology
- Due diligence
- Contract/Services Review
- Monitoring
- Termination

Signs of an Ineffective Program

How Does Your Organization Rate?

LACK OF STAKEHOLDER SUPPORT: DEPARTMENTS NOT WORKING TOGETHER WITH THE TEAM EXECUTING, WILL FAIL.

GENERIC QUESTIONNAIRES: SHOULD BE TAILORED TO SERVICES AND RESPONSES SHOULD BE REVIEWED BY QUALIFIED INDIVIDUALS.



SPLIT VENDOR REVIEW PROCESS: NEEDS TO BE COHESIVE.

VENDOR TOOLS INADEQUATE: LIMITED FUNCTIONALITY OR PURCHASED PRIOR TO PROGRAM DEVELOPMENT.

LIMITED TRANSPARENCY WITH VENDOR: KEY IS COMMUNICATION.

NONEFFECTIVE REVIEWS OF SOC2 REPORTS.

Machelle Rinko, CPA, CIA, CFIRS
Internal Audit & Risk Management Consultant
Machelle.Rinko@gamail.com
M: 330.501.3474

Elizabeth Namanny, JD, MBA
Wealth Management Finance & Risk Officer
Trustmark National Bank
enamanny@trustmark.com
O: 601.208.2406

Trustmark National Bank is not directly affiliated with the co-presenter or the sponsoring organization.