STRATEGIES FOR OPTIMIZING THIRD-PARTY RISK MANAGEMENT

Casey Ryder - VP, Operational Risk Manager

Boston Private Bank & Trust

AGENDA

- INTRODUCTION
- BUILDING A PROGRAM AND FRAMEWORK
- ASSESSING YOUR THIRD PARTIES
- DON'T FORGET ABOUT FOURTH PARTIES
- REPORTING TO SENIOR EXECUTIVES / BOARD
- PARTNERSHIPS AND EDUCATION
- OVERCOMING RESOURCE AND BUDGET LIMITATIONS
- KEY TAKEAWAYS

BOSTON PRIVATE

WEALTH ▫ TRUST ▫ PRIVATE BANKING

Introduction

Evolving Third Party and Threat Landscapes

Digital transformations, cloud migrations, IoT, and “nth” parties (subcontractors) have made third party engagements more complex.

Cyberattacks and security incidents are routinely attributed to third parties with weak security practices

Increased Regulatory Scrutiny

Regulatory and compliance requirements for third-party oversight are increasing on a local, federal and international level with the potential for significant fines

Expanding Operational Risks

The operational risk landscape is changing.

Climate change, pandemics, digitization, globalization, high profile customer disruptions and regulatory fines all contribute to elevated operational risks.

Legacy Programs No Longer Enough

Traditional TPRM programs are no longer a match for the realities of the modern third-party risk landscape

“One-size-fits-all” questionnaires, point in time assessments and siloed efforts are no longer effective strategies.

BOSTON PRIVATE
WEALTH ▫ TRUST ▫ PRIVATE BANKING

Building a Program and Framework

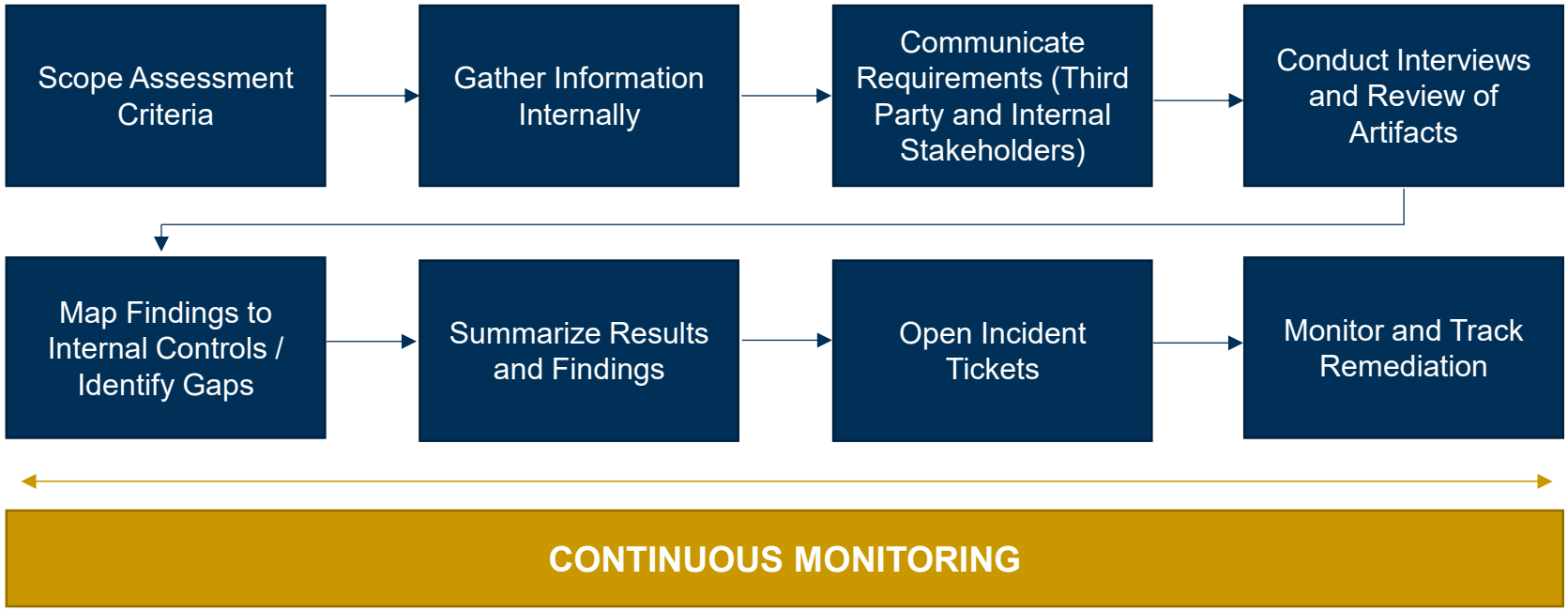
- **Establish a governance framework** and treat third-party risk management as a cross-functional effort by involving stakeholders and subject matter experts throughout your organization. Leverage the “three lines of defense” model.
- **Develop a policy and program** that defines key elements, outlines roles and responsibilities, and is aligned with key business objectives and strategies
- **Develop scoping criteria** and categorize your third parties by inherent risk

Data	**Data Elements**
	Data Location
	Transmission Method(s)
System Access	**Applications / Network Connections**
	System Integrations
	Remote Access
Continuity and Recovery	**Business and user impact (RTO & RPO)**
	Revenue impact
Compliance	**Impact on local, federal or international regulations**

- **Establish due diligence criteria** based on inherent risk
- **Develop strong contracts** that outline the rights and responsibilities of all parties and protect your organization

BOSTON PRIVATE
WEALTH ▫ TRUST ▫ PRIVATE BANKING

Assessing Your Third Parties



- Derogatory news monitoring
- Periodic financial / credit analyses
- Performance monitoring against SLAs
- Issue management (monitoring and tracking)
- Vendor advisory feeds
- Security monitoring tools

BOSTON PRIVATE
WEALTH ▫ TRUST ▫ PRIVATE BANKING

Don’t Forget About Fourth Parties

Contractual Provisions

Contractually bind your third parties to inform and obtain your approval on fourth party / subcontractor usage.

Identification

Identify fourth party involvement as it relates to your third-party engagements.

Develop an inventory of all fourth parties by product or service offered as well as location (U.S. and offshore).

Oversight

Gather and manage information on fourth parties as part of the third-party oversight process.

Ensure fourth parties are included in the scope of screening and risk management processes.

Reporting

Issues identified during screening process

Concentration risk

Geographic risk

BOSTON PRIVATE
WEALTH ▫ TRUST ▫ PRIVATE BANKING

Reporting to Senior Executives / Board

Risk Measure	Metric / KPI / KRI	Metric Objective
Third Party Landscape	# Third parties by risk rating	Trending on which risk levels are increasing over time
	# Third parties by location (onshore vs. offshore)	Trending on whether use of foreign-based service providers is increasing
	Third-party spend	Identify highest spend to maximize value from third parties
	# Red flags / issues identified	Trending on issues identified through continuous monitoring and whether critical issues are increasing over time
Program Health	# third party reviews by quarter	Insight into how the third party portfolio is being managed and overseen
	Review status by quarter (i.e. completed, not started, on hold, etc.)	Insight into whether resource levels are sufficient
	Average days to review	Insight into whether resource levels are sufficient
Awareness	# of third parties on-boarded outside of the Program	Insight into whether the organization understands which third parties are in-scope and whether additional education is required

BOSTON PRIVATE
WEALTH ▫ TRUST ▫ PRIVATE BANKING

Partnerships and Education

- **Tone from the Top**
  - Senior management, including the C-suite and Board, are accountable for the risks in third-party relationships. It is their responsibility to create a culture of transparency and collaboration, while also identifying and controlling the risks that arise from third-party relationships.

- **Stakeholder and Subject Matter Expert (SME) Partnerships**
  - Align your TPRM program with those throughout your organization who have a vested interest. Ensure collaboration.

- **Training and Awareness**
  - Educate the organization, especially those individuals directly managing third-party relationships. You are only as good as the information you have.

- **Third Party Partnerships**
  - Treat your third party relationships as partnerships and ensure the lines of communication are always open. Enhance organizational value by partnering with third parties who can act as SMEs or trusted advisors to focus on strategic agility, innovation, performance improvement, and risk mitigation / reduction.

BOSTON PRIVATE
WEALTH ▫ TRUST ▫ PRIVATE BANKING

Overcoming Resource and Budget Limitations

- **Determine which third-party engagements pose the most risk to your organization by developing scoping criteria appropriate to your organization. Tailor or customize your due diligence assessments rather than following a one-size fits-all approach.**

- **Conduct virtual (“desktop”) assessments unless an onsite visit is required**

- **Leverage free resources to enhance your continuous monitoring:**
  - Google Alerts for negative news monitoring
  - States attorney general and Better Business Bureau websites
  - Security and vulnerability databases and subscriptions
    - Computer Emergency Readiness Team Coordination Center (CERT/CC)
    - US-Cert
    - National Vulnerability Database
  - Vendor Advisory Feeds

BOSTON PRIVATE
WEALTH ▫ TRUST ▫ PRIVATE BANKING

Key Takeaways

- **Establish governance processes and build out a framework which defines the third-party risk program, roles and responsibilities, and is aligned with business objectives.**
- **Create strong contracts that will protect your organization, outline the responsibilities of all parties, with performance and service level expectations.**
- **Partner with subject matter experts and stakeholders to sell the benefits of third-party risk management and ensure a supportive tone from the top.**
- **Encourage ongoing training and awareness throughout your organization and monitor compliance with the program.**
- **Partner with your third parties to ensure the lines of communication are always open.**
- **Identify key metrics which will inform on your program's health as well as key risks that pose a threat to your organization.**

BOSTON PRIVATE
WEALTH ▫ TRUST ▫ PRIVATE BANKING