Third-Party Risk Management
Three Lines of Defense Model

Center for Financial Professionals

How the three lines of defense (LoDs) model is impacting third-party risk management

- Subject Matter Experts (SME) vs Risk Management domains
- Roles and Responsibilities
- 1st Line of Defense - Third Party Relationship Management
- 1st Line of Defense - Third Party Assessments
- 2nd Line of Defense - Policies and Guidance
- 2nd Line of Defense - Review and Challenge
- 3rd Line of Defense - Internal Audit
- The 1.5 Line of Defense position
- TPRM alignment within the evolving Three Lines of Defense Model

Subject Matter Experts (SME) vs Risk Management domains

- The 1st line of defense (LoD) owns the risk of using third parties
- The 2nd LoD owns establishment of risk controls needed to address risk.
- The 2nd LoD Risk Management domains includes:
  - Operational Risk (including TPRM)
  - Compliance Risk Management
  - Information Risk Management
  - Model Risk Management, etc.
- The 1st LoD owns the SMEs who assess controls related the risk domains established by 2nd LoD Risk Management

Center for Financial Professionals

Roles and Responsibilities

- Need for a clear definition and ownership of roles and responsibilities
- Need to delineate between 1st and 2nd LoD functions
- Need to have a path to escalate and resolve issues

1st LoD - Third Party Relationship Management

1. The Business owns the risk associated with using a third party
2. 1st LoD TPRM is responsible for
   - assisting relationship owners with managing higher risk relationships
   - Reporting on the risk profile related to the use of third parties
   - Working with the Business' risk management teams to mitigate third party risk
   - Working with 1st LoD SMEs to understand and mitigate risks identified through third party SME assessments
   - Coordinating with other 1st LoD TPRM resources who also use the third party
   - Ensuring accurate, timely, and complete information is captured is the system of record
   - Complying with the TPRM Program as documented by the 2nd LoD

1st LoD - Third Party Assessments

- The Business owns the risk associated with using a third party
- 1st LoD SMEs areas responsible for
  - Performing third party control assessments, for their respective risk areas
  - Complying with the standard and guidance issued by their 2nd LoD Risk Management areas
  - Complying with their established service level agreements
  - Identifying the severity of any third party control deficiency
  - Working with the Business and 1st LoD TPRM to determine an acceptable path forward (e.g., remediation plans, risk acceptance, termination of the relationship, etc.)

Center for Financial Professionals

2nd LoD - Policies and Guidance

- 2nd LoD TPRM is responsible for the following areas:
  - In collaboration with the 1st LoD TPRM and SMEs and other 2nd LoD Risk Management areas, establish TPRM Policy , Procedures, guidance, target operating model, and governance for the enterprise TPRM Program
  - Creating and deploying training and ensuring communications related to the TPRM Program occur in a timely manner
  - Developing and maintaining a TPRM technology solution that meets the requirements of TPRM stakeholders and provides workflow, controls, approvals, and reporting capabilities to comply with the TPRM Program
  - Ensure that the population of third parties is appropriately inventoried from a risk perspective
  - Ensure that the population of Legal Entities (aka Affiliates) are appropriately included within the enterprise TPRM Program
  - Establishing TPRM Risk Appetite Metrics

2nd LoD - Review and Challenge

- 2nd LoD TPRM Review and Challenge is responsible for the following :
  - In collaboration with the 1st LoD TPRM and SMEs and other 2nd LoD Risk Management areas, establish the approach, process, workflow, reporting, and escalation needed to appropriately review and challenge the work of TPRM key stakeholders
  - Determining the scope and thresholds needed to determine TPRM Program effectiveness
  - Determine whether corrective actions are necessary for identified issues, and track them to closure, as required
  - Determining sampling methodology across portfolios and Entities

3rd LoD - Internal Audit

- 3rd LoD Internal Audit responsible for the following :
  - Independently assessing the enterprise TPRM Program
  - Independently assessing if key stakeholders are complying with published Policies, Procedures, and Guidance
  - Independently assessing the effectiveness and sustainability of the TPRM Program
  - Independently assessing the quality, accuracy, and completeness of reporting and data contained within the system of record
  - Providing findings, observations, and recommendation to 1st and 2nd LoD TPRM Management regarding the TPRM Program and it execution
  - Independently providing validation of submission packages related to resolution of Regulatory items

Center for Financial Professionals

The 1.5 LoD position

- A number of areas have been defined as a “1.5 LoD” including: Compliance, Contracting, Business Continuity, Legal, Human Resources, etc.
- This “1.5 LoD” occurs for two principle reasons
  - The organization has a single group that performs their work within the business and also establishes it own processes and guidance
  - The organization is too small to be able to create separate 1st and 2nd LODs

TPRM alignment within the evolving Three Lines of Defense Model

- The trend is to establish compliant 1st and 2nd LoDs
- Where Affiliates are involved, the central, enterprise group, may take on the 2nd LoD function and the Affiliate org take on the 1st LoD functions. And the 1st LoD may use a Risk Function resource, not directly involved with the relationship, to perform the Business Unit Risk function
- As an interim solution a TPRM Review and Challenge team may be staffed with resources who are knowledgeable in other risk areas (e.g., Information Security, Business Continuity, etc.) to assist in the independent review and challenge of the 1st LoD SME efforts until the formal 2nd LoD Risk Management function is established

Questions?