CastleHill

MANAGED RISK SOLUTIONS

Embracing a Siloed Approach to TPRM

Embracing a Siloed Approach to TPRM

- Use Case for a Siloed Approach
- Why do we use silos
- Rationalizing the Silo Option
- Why is TPRM Different
- Prioritization – Develop the Baselines

Embracing a Siloed Approach to TPRM

If you're a small or mid-tier organization with **time sensitive** regulatory pressure or **limited "Top Down" GRC support**, there are strong arguments for the efficiency and practicality of implementing **Third-Party Risk Management** capability as a **siloed function**. This discussion addresses the use case, rationalization, prioritization and opportunities aligned to introducing supportable program policies, data driven process and other powerful **baseline** Vendor Risk Management capabilities in small TPRM teams. Leverage these TPRM capabilities to act as Enterprise influencers, pushing risk management culture and best practice from the bottom up. Understand the maturity process that grows a siloed TPRM organization from **Service Provider status to Enterprise Business Partner** and Leader.

Use Case for a Siloed Approach

When You Have This

- A Mandate
- Limited Executive Leadership
- Identified but Limited Stakeholders
- Basic Capability and Process
- Baseline Requirements
- Limited Resources and Relationships
- Excellent Soft Skills

...But Not This

- Existing Well Defined Program
- Mandatory Buy-In
- Vocal Organizational Leadership
- Enterprise Risk Drivers
- Many Resources and Relationships
- Engaged Stakeholders
- Well Defined Requirements

Metaphor Fun - Why do farmers use silos?

- Silos are feeder systems that meter both resource inputs and outputs
- Silos are insulated and provide resources with protection from pests and bad weather
- Silos prevent cross contamination internally and externally
- When the barn burns down, silos protect the resources that keep critical operations going

Rationalizing the Silo Option

Point

The disadvantages of the silo mentality, are that it shortcuts collaboration, saps morale, curtails productivity, creates organizational dysfunction, and sends mixed signals.

Counter Point

This was true over the past several decades when elimination of silos, was necessary in refactoring workforce efficiency. Better technology, communication and business practices mitigate many of the issues from 40 years ago.

Rationalizing the Silo Option

Point

We would develop a “silo mentality”. TPRM would operate in the shadows and become a law unto itself.

Counter Point

TPRM is an Internal Customer Service function. Limited well defined scope and the development of internal relationships means communications and process support provide excellent transparency.

Rationalizing the Silo Option

Point

Accountability rests individual siloed functions to ensure they get the skills and resources they need to function effectively. Resources and skillset would be duplicated.

Counter Point

The TPRM skillset is domain specific and not generally shared across an enterprise. TPRM is only very rarely, a duplicated internal function.

Rationalizing the Silo Option: A Note on Collaboration

Action VS Inaction

Within a silo it's much easier to define and implement a high priority initiative or outcome quickly

Enterprise Collaboration can be "disabling" in a large organization and in some cases become an excuse for not acting

"When you need 30 people to say 'yes' for an idea to proceed, but you only need one to say 'no' for everything to come to a halt, that's when the well-intentioned desire for collaboration can lead to inaction." ~ Abraham Lincoln *(Not Really)*

TPRM is Different…

Isolating TPRM Means Limited Stakeholder Requirements - Third-Party Risk Management is generally a centralized function that leverages very specific and limited line of business partnerships and Subject Matter Experts to address capability gaps.

TPRM On Its Own, Requires a Low Overhead Technology Footprint - TPRM is a "Net Data Exporter" of specialized information and requires little internal data support (usually metadata only) to be highly effective. Also, TPRM does not require broad Enterprise integration for the data to be high quality or highly available, only a reporting solution that accepts TPRM data.

Siloed TPRM Addresses Enterprise Security Considerations - Effective TPRM requires direct interaction with external Service Providers with access to internally leveraged platforms; platforms that should be carefully segregated from Enterprise infrastructure.

Standalone TPRM Programs Provide Significant Automation - TPRM tools (technology solutions) are highly available, mature and most are low overhead. Requirement that force TPRM into existing enterprise tools , generally destroys TPRM value, creates artificial dependencies and ultimately forces a paradigm that is inconsistent with maintaining an efficient and effective TPRM program.

Prioritization – Develop the Baselines

Define your baseline objectives, the inputs and outputs:

Support Strategic Objectives

Support Stakeholder Requirements

Develop Baseline Capability

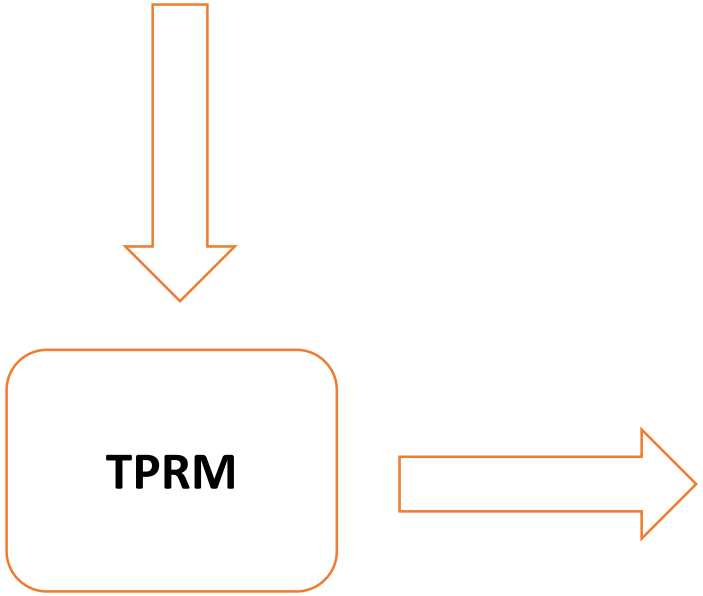
Collect Vendor Data

Leverage Vendor Data

Inputs:

Vendor Business Data

Vendor Risk Data



Outputs:

Inherent Risks

Materiality/Criticality

Residual Risks

Classification and Cadence

Prioritization – Develop the Baselines

Document your baseline Third-Party Risk Management Program:

Identify the Mission, Inputs and Outputs

Show Governance

Discuss Partnerships and Integration

Explain the Framework, Roles and Responsibilities

Expose the Process

Do Not Include:

Policies or Policy Statements, Training Documentation, or Non-TPRM Process

Document the baseline process map showing timelines and process handoffs:

Pro Tip - Keep it Simple

Define Process Handoffs Explicitly, along with the Roles and Responsibilities for All Actors

Define the Timeline for Each Process Segment

Pit falls:

Creating Chokepoints and Artificial Dependencies

Soft Handoffs – DATA DRIVES PROCESS

Prioritization – Develop the Baselines

Establish Governance leveraging a few stakeholders and a representative from each contributing team:

Stay in Control -Leverage Your Silo to Keep Things Manageable

Establish a Clear Mission and Solid Scope

Participation: Solicit Participants Who Have “skin in the game” Only

Pit Falls:

Exceeding Scope and Managing Exceptions Outside of Policy (favoritism)

Including Interested Parties Without a Vested Interest in the Outcomes

Document baseline Policy with content aligned to the TPRM Program requirements and related business process only:

Create Policy only for TPRM Program specific concerns

Keep Policy Small – Who, What, How, When

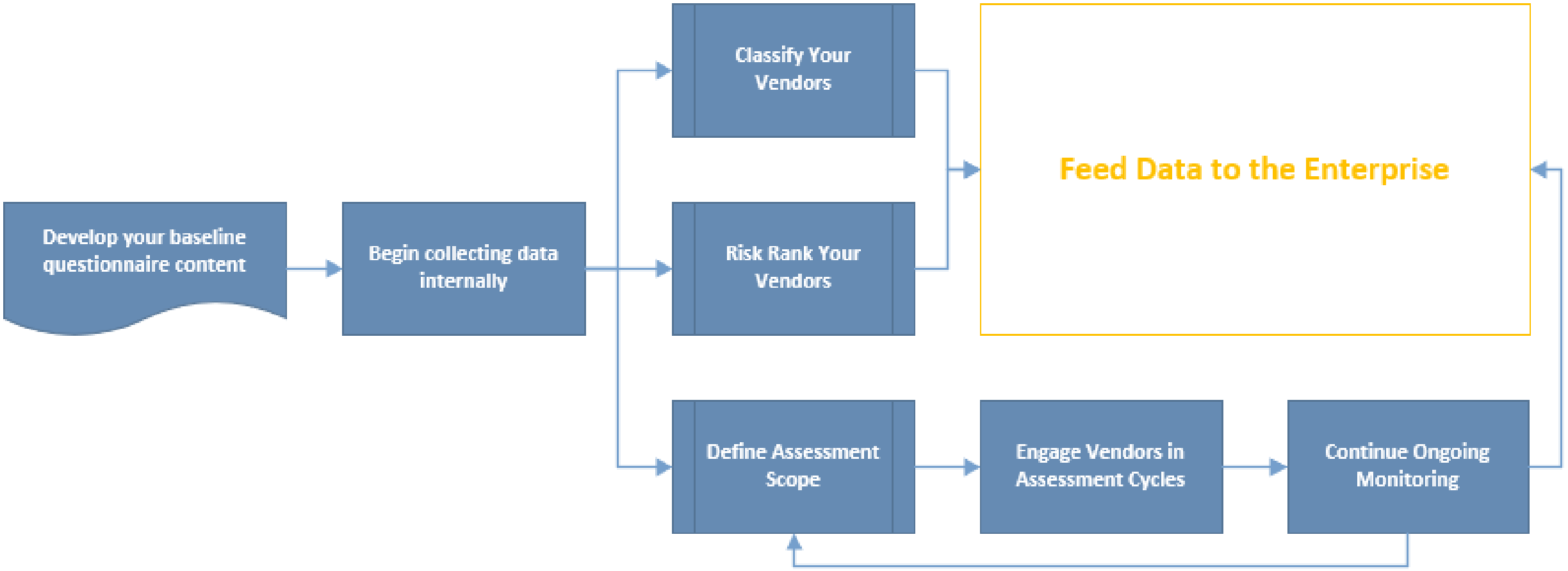
Reinforce Timelines (Internal SLAs)

Pit Falls:

Policy Scope Creep – Stay Focused!

Avoid Narratives and Discussion Within the Documents – Avoid the Appearance of Loopholes

Prioritization – Execute Capability



Remember…

When the conditions are right, embracing a silo mentality enables implementation of a high priority initiative or outcome quickly

Questions?