TPRA

THIRD PARTY RISK ASSOCIATION

September’s Practitioner Meeting

Julie Gaiaschi, CEO & Co-Founder

For your awareness, this call is being recorded

THIRD PARTY
RISK ASSOCIATION

AGENDA

- Opening Remarks
- Roundtable: Back to Basics – Building an Effective TPRM Program
  - Planning and Oversight
  - Pre-Contract Due Diligence
  - Contracting
  - Continuous Monitoring
  - Disengagement
  - Continuous Improvement
- Closing Remarks

TPRA | THIRD PARTY RISK ASSOCIATION

Opening Remarks:

- **9/22 - Focus Group Call** @ 10 AM Central – Topic: InfoSecurity Questionnaire
- **9/27 - Women in TPRM** Meeting @ 1 PM Central – Join a working group online!
- **September - Launching our Practitioner Year-End Survey!** For participating, you will be entered into a raffle for a $100 Amazon gift card or a TPRA account upgrade to a Premium Membership (which includes your ticket to our in-person conference)!
- **YouTube** Channel – Subscribe to Third Party Risk Association
- **Slack Space Forum** – Join under “Member Services” using the “Slack Forum” link.
- Join our **LinkedIn Page** to view upcoming events and promotional opportunities.

TPRA Certifications Program – Launching This Month!

TPRA THIRD PARTY RISK ASSOCIATION

Third Party Cyber Risk Assessor© (TPCRA©) Certification

The TPCRA Certification is a specialized qualification designation to confirm your understanding and skill in the assessment of third party cyber security controls and processes, as well as validate your competency in the creation, execution, and management of third party cyber risk assessments.

The **first 30 individuals** that register will receive the book "Cybersecurity & Third Party Risk", a signed bookmark by the author Greg Rasner, and 30 days of access to Greg himself!

TPRA THIRD PARTY RISK ASSOCIATION

Fall Virtual Conference

- Theme: "**Back to Basics - Building an Effective TPRM Program**"
- Date: Monday, October 17th through Friday, October 21st from 10 AM to 2 PM Central each day
- Cost: FREE for TPRA Members & Non-Members
- Agenda:
  - Monday - TPRM Oversight
  - Tuesday - Pre-Contract Due Diligence
  - Wednesday – Contracting
  - Thursday - Continuous Monitoring
  - Friday – Disengagement
- Will include up to 15 hours of Continuing Professional Education (CPE) credits.

THIRD PARTY RISK ROUNDUP

April 24 - 26, 2023

Nashville Marriott at Vanderbilt University
2555 West End Ave
Nashville, Tennessee

www.thirdpartyriskroundup.org

VIP Network Experience invites will go to the first 40 Practitioners that register.

Call for Speakers & Sponsors is now OPEN!

TPRA | THIRD PARTY RISK ASSOCIATION

GRF Summit - Security & Third Party Risk

- Date: Thursday, October 27th & Friday, October 28th
- Location: Gaylord National Resort, National Harbor Maryland
- Agenda: Sessions will cover risk and vendor management, cybersecurity, intelligence sharing, geopolitical threat mitigation, and emerging compliance/regulation.
- To register, visit www.grf.org/summit/2022/overview or you can visit TPRA's External Events page.
- Find our Booth at the event and say "Round-up VIP" to receive a VIP Network Experience invite for our Spring in-person conference!

THIRD PARTY RISK ASSOCIATION

Roundtable: Back to Basics – Building an Effective TPRM Program

TPRA THIRD PARTY RISK ASSOCIATION

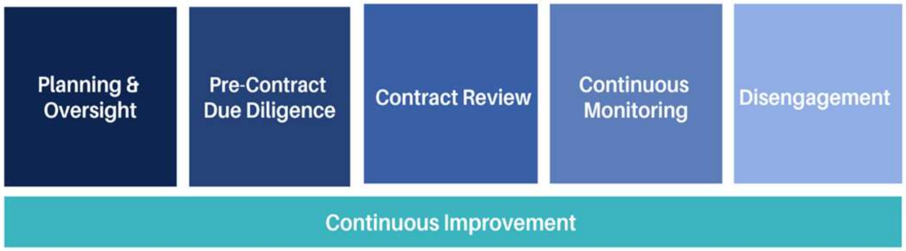
What is Third Party Risk Management?

- **Third Party** will be broadly defined to include all entities that can or do provide products and/or services to an organization regardless as to whether a contract is in place or monies are exchanged (e.g. Affiliates, Subsidiaries, Consultants, Contractors, Sub-Contractors, Vendors, Service and Solution Providers, Fourth parties, and more).
- **Third Party Risk** is the possibility of an adverse impact on an organization's data, financials, operations, reputation, or other business objectives, as a direct or indirect result of an organization's third party.
- **Risk** is equal to the level (impact) times likelihood that a risk will occur. Risk can be inherent (before controls are considered) or residual (after controls are considered).
- **Control** is a process and/or activity used to monitor, review, or address a specific risk.
- **Third Party Risk Management (TPRM)** is the framework that consists of policies and procedures, controls, and oversight; established to identify and address risks presented to an organization by their third parties.

Why is TPRM Important?

- Historically, organizations procured services from third parties for cost efficiency purposes.
- Today, the purpose of procuring third party products and services has greatly evolved. Now, it includes, but is not limited to, outsourcing critical processes, quickly scaling services to reach global markets, focusing on more strategic priorities, reaching niche markets, and gaining additional expertise and functionality. With this evolution comes increased risk and impact that third parties can pose to organizations.
- To ensure third parties are operating securely and effectively, by adequately monitoring and mitigating risks related to the data and/or processes that have been outsourced, an organization must have in place an effective TPRM program.
- While there is no way to eliminate the risk of a data breach or verified incident, there are security measures that can be taken by the organization to ensure they understand the risk of working with the third party and take appropriate steps to mitigate the risk.
- Failure to appropriately measure and manage the risks that come along with entering into a relationship with a third party can cause organizations to face scrutiny from their regulators, subject them to fines and other legal repercussions, or cause major reputational or financial risk.

THIRD PARTY RISK ASSOCIATION



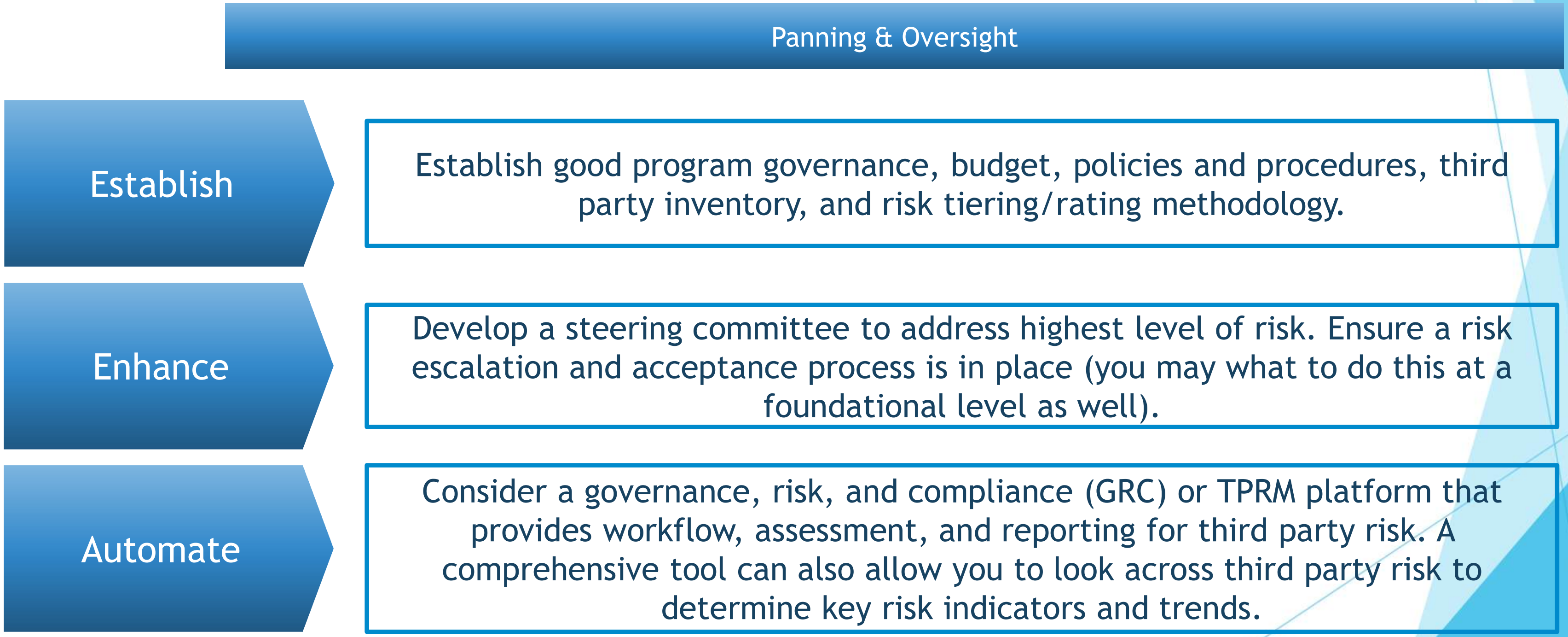
TPRM Program Lifecycle

Generally, most TPRM programs include the following activities:

- **Planning and Oversight** – Provides an organization with the foundation to build upon and properly support their overall program.
- **Pre-Contract Due Diligence** – Ensures the organization performs due diligence, commensurate with the level of inherent risk, to determine if the organization should proceed with a specific third party relationship and prior to signing a contract. This phase assists with determining if a third party meets business needs in context of the risk presented.
- **Contract Review -** Ensures the organization documents relationship expectations in an agreement that can be upheld in a court of law. It also ensures risks noted within the due diligence process can be addressed within contractual clauses.
- **Continuous Monitoring -** Requires the organization to assess third party risk on a continual basis to ensure contract terms, business obligations, legal and regulatory requirements, and performance expectations are met.
- **Disengagement** – Ensures the organization is able to transition away from a third party with minimal impact should the relationship end due to contract expiration or adverse/unplanned conditions are met.
- **Continuous Improvement** – Is an ongoing activity which seeks to enhance the organization’s TPRM program as third party risk management guidance, trends, and techniques are realized.

TPRA THIRD PARTY RISK ASSOCIATION

Planning & Oversight



Panning & Oversight

Establish

Establish good program governance, budget, policies and procedures, third party inventory, and risk tiering/rating methodology.

Enhance

Develop a steering committee to address highest level of risk. Ensure a risk escalation and acceptance process is in place (you may what to do this at a foundational level as well).

Automate

Consider a governance, risk, and compliance (GRC) or TPRM platform that provides workflow, assessment, and reporting for third party risk. A comprehensive tool can also allow you to look across third party risk to determine key risk indicators and trends.

TPRA THIRD PARTY RISK ASSOCIATION

Due Diligence

Due Diligence

Establish

Integrate into the Procurement process and ensure due diligence/risk assessment reviews are performed before contracts are signed. Ensure you have a risk-based approach by running your third parties through an Inherent Risk Questionnaire (IRQ).

Enhance

Ensure you have a seat at the table with those making third party risk-based decisions, such as Procurement, Legal, Compliance, and others. Actively participating in conversations will ensure your program gains the support it needs, as well as ensures you are able to obtain the necessary evidence and documentation to perform your reviews.

Automate

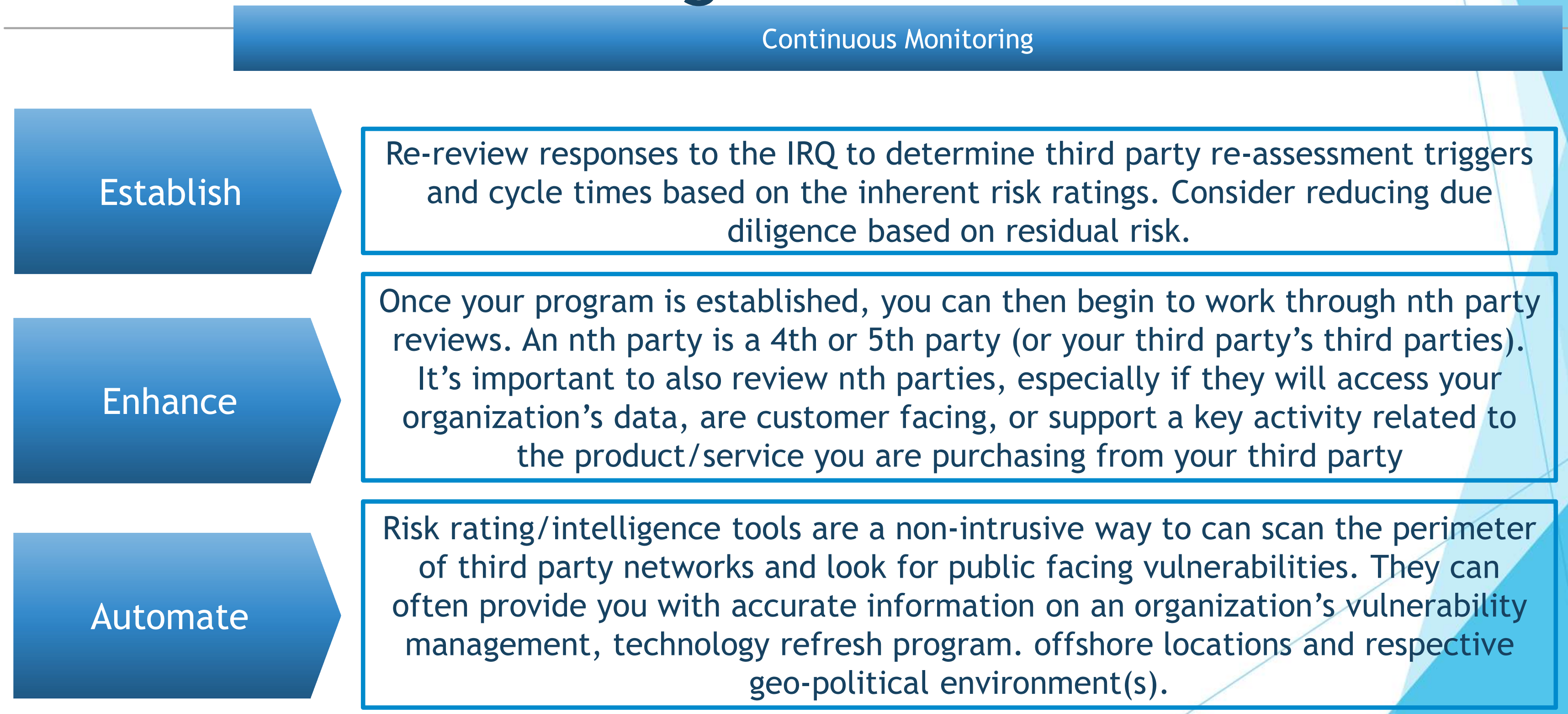
A GRC or TPRM platform can also assist with automating the questionnaire process and allow you to obtain evidence quicker during the pre-contract due diligence phase. You may also consider joining a third party risk assessment collective (where third parties share the responses to one questionnaire with several organizations) to assist with third party response time

Contracting

	Contracting
Establish	Develop a contract template that defines expectation of third party controls that need to be in place, as well as allow for the review of said controls by your organization.
Enhance	You may want to “own” certain contract clauses to ensure that any redlines to specific clauses are reviewed by your team. Small changes could affect what evidence you receive from third parties and how you can assess them. You may also want to add noncompliance triggers to your contracts. These triggers ensure you can take action against contract non-compliance.
Automate	Consider implementing a tool that will notify you when contracts are no longer in compliance with updated contract templates. This helps you ensure that you are maintaining contract compliance with your third parties.

TPRA THIRD PARTY RISK ASSOCIATION

Continuous Monitoring



Continuous Monitoring

Establish

Re-review responses to the IRQ to determine third party re-assessment triggers and cycle times based on the inherent risk ratings. Consider reducing due diligence based on residual risk.

Enhance

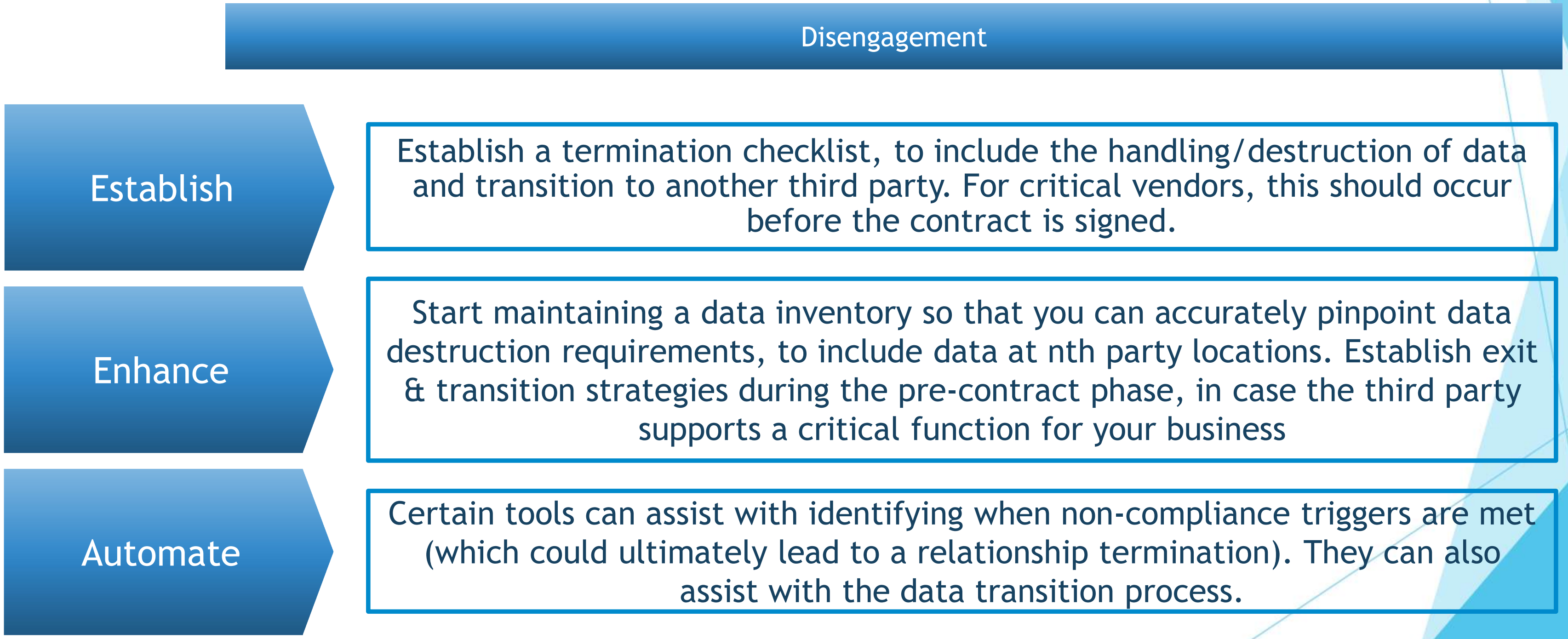
Once your program is established, you can then begin to work through nth party reviews. An nth party is a 4th or 5th party (or your third party's third parties). It's important to also review nth parties, especially if they will access your organization's data, are customer facing, or support a key activity related to the product/service you are purchasing from your third party

Automate

Risk rating/intelligence tools are a non-intrusive way to can scan the perimeter of third party networks and look for public facing vulnerabilities. They can often provide you with accurate information on an organization's vulnerability management, technology refresh program. offshore locations and respective geo-political environment(s).

THIRD PARTY RISK ASSOCIATION

Disengagement



Disengagement

Establish

Establish a termination checklist, to include the handling/destruction of data and transition to another third party. For critical vendors, this should occur before the contract is signed.

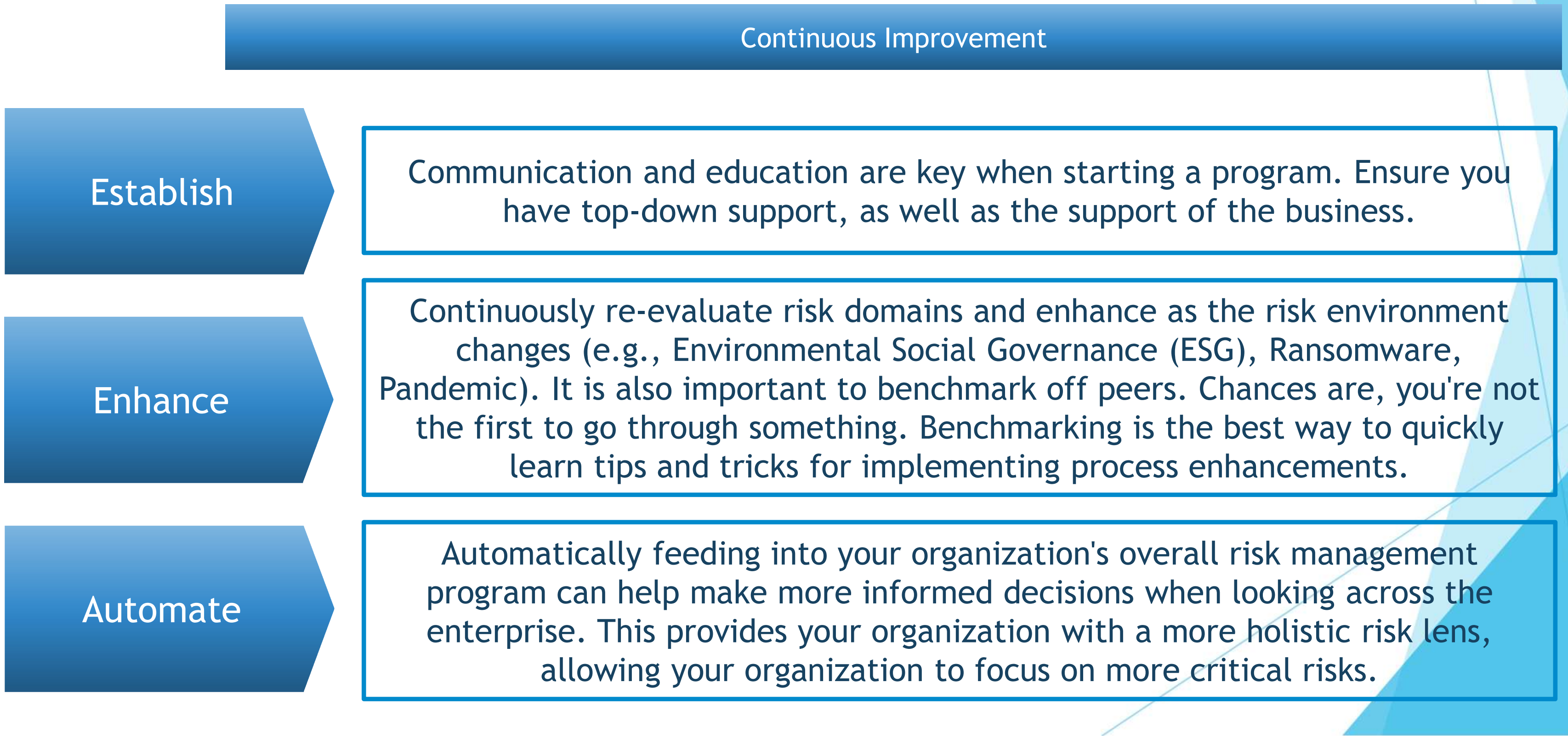
Enhance

Start maintaining a data inventory so that you can accurately pinpoint data destruction requirements, to include data at nth party locations. Establish exit & transition strategies during the pre-contract phase, in case the third party supports a critical function for your business

Automate

Certain tools can assist with identifying when non-compliance triggers are met (which could ultimately lead to a relationship termination). They can also assist with the data transition process.

Continuous Improvement



Continuous Improvement

Establish

Communication and education are key when starting a program. Ensure you have top-down support, as well as the support of the business.

Enhance

Continuously re-evaluate risk domains and enhance as the risk environment changes (e.g., Environmental Social Governance (ESG), Ransomware, Pandemic). It is also important to benchmark off peers. Chances are, you're not the first to go through something. Benchmarking is the best way to quickly learn tips and tricks for implementing process enhancements.

Automate

Automatically feeding into your organization's overall risk management program can help make more informed decisions when looking across the enterprise. This provides your organization with a more holistic risk lens, allowing your organization to focus on more critical risks.

TPRA THIRD PARTY RISK ASSOCIATION

Value of a TPRM Program

- Holistic risk lens into risk landscape.
- Able to proactively mitigate and address third party risk in a timely manner.
- Ability to meet Regulator and Board expectations.
- Stay up to date on risk trends and ensure your program is flexible enough to incorporate where needed.
- Save time and resources while focusing efforts on addressing higher risk.

TPRA THIRD PARTY RISK ASSOCIATION

TOOL TALK

WITH

ARAVO

TPRA THIRD PARTY RISK ASSOCIATION

Next Meeting: Thursday, October 13th from 10 to 11:00 AM CST

Topic: TPRM Budgeting (Considerations, Showing Value, Tools, Resources, Training)

Thank you for joining!